RSAC 2025 Conference

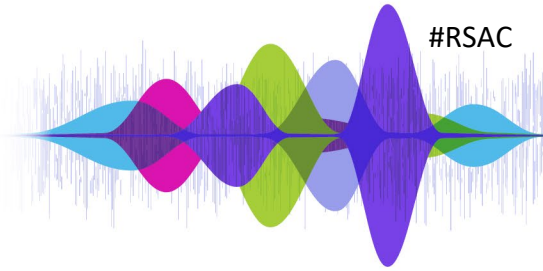
Many Voices.
One Community.

SESSION ID: GRC-M06

Dismantle the Three Lines of Defense: Embrace Continuous Risk Management!

Alla Valente
Principal Analyst
Forrester Research
https://www.linkedin.com/in/allavalente/

Cody Scott
Senior Analyst
Forrester Research
https://www.linkedin.com/in/codyscott/



Disclaimer

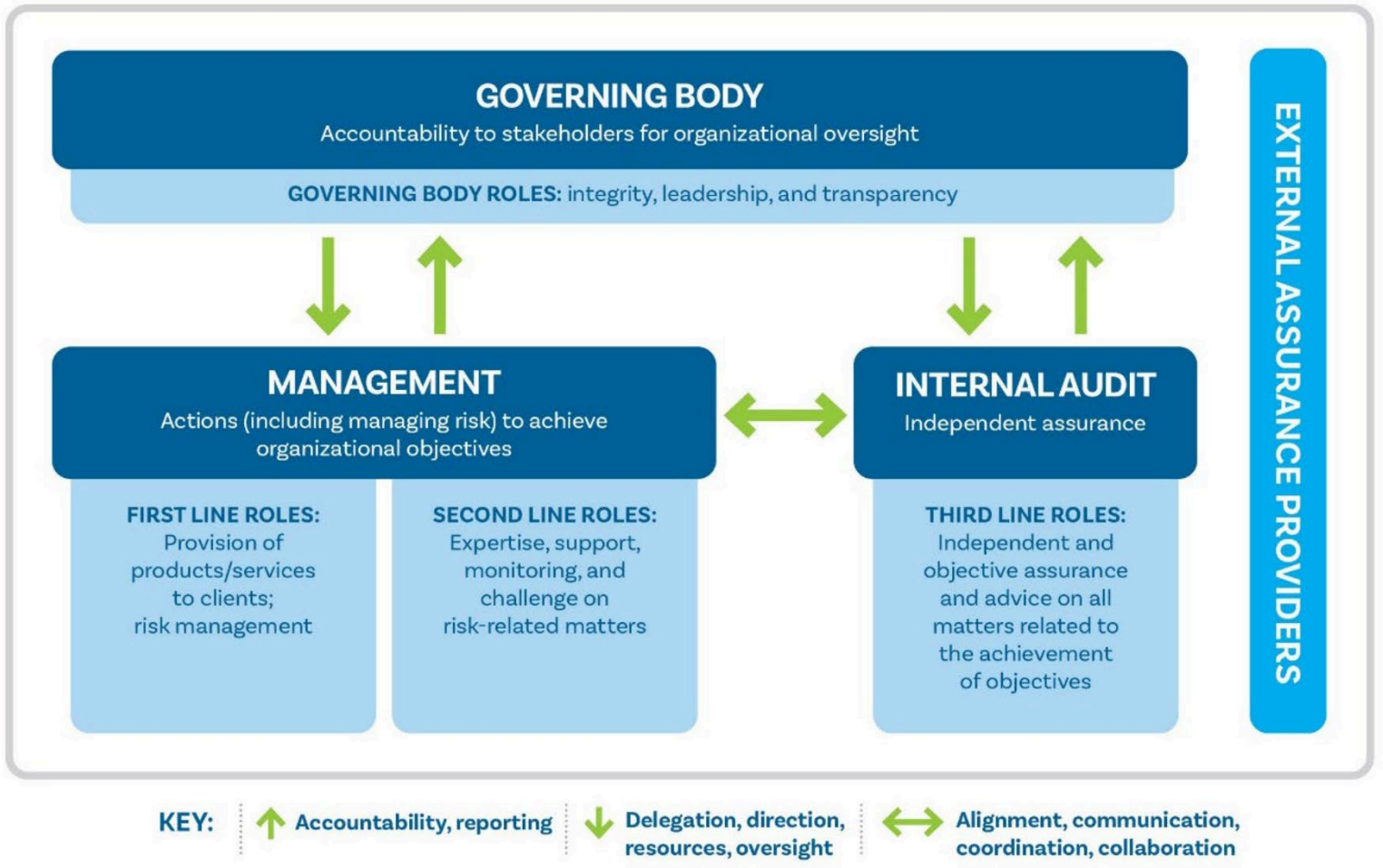
Presentations are intended for educational purposes only and do not replace independent professional judgment. Statements of fact and opinions expressed are those of the presenters individually and, unless expressly stated to the contrary, are not the opinion or position of RSA Conference LLC or any other co-sponsors. RSA Conference LLC does not endorse or approve, and assumes no responsibility for, the content, accuracy or completeness of the information presented.

Attendees should note that sessions may be audio- or video-recorded and may be published in various media, including print, audio and video formats without further notice. The presentation template and any media capture are subject to copyright protection.

© 2025 RSA Conference LLC or its affiliates. The RSAC and RSAC CONFERENCE logos and other trademarks are proprietary. All rights reserved.

THREE LINES OF DEFENSE

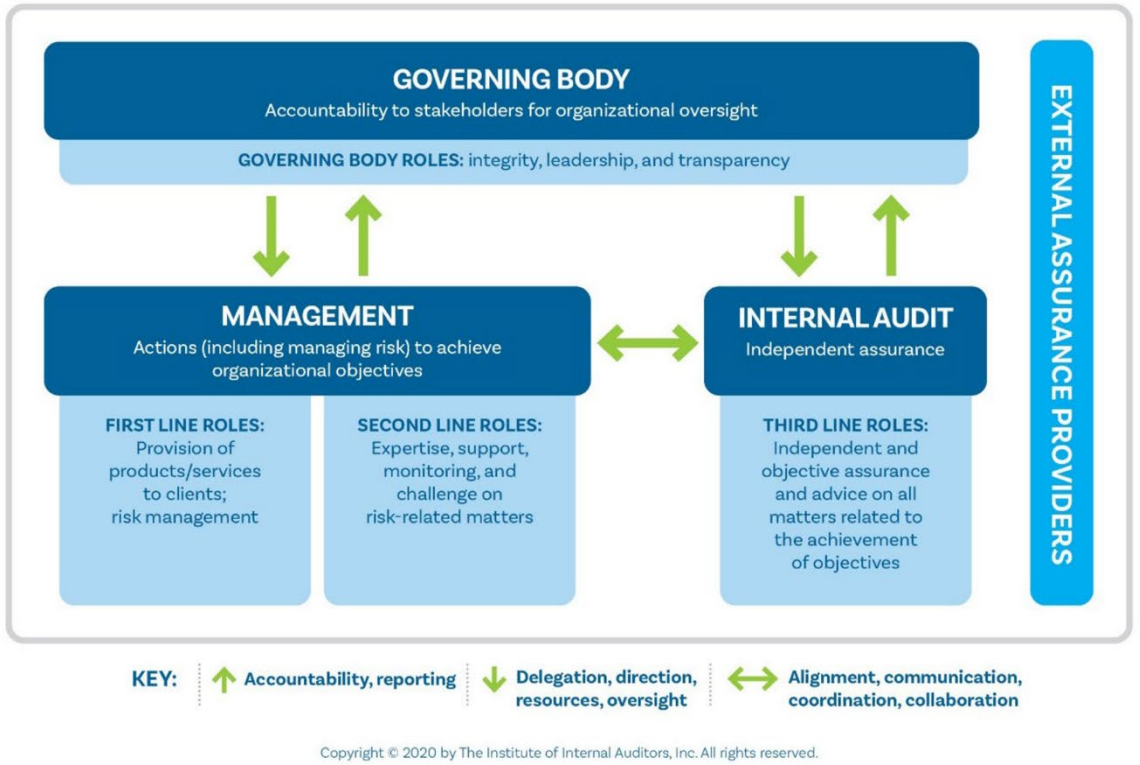
Three Lines Of Defense (3LoD) Model


GOVERNING BODY
Accountability to stakeholders for organizational oversight
GOVERNING BODY ROLES: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
INTERNAL AUDIT
Independent assurance
FIRST LINE ROLES: Provision of products/services to clients; risk management
SECOND LINE ROLES: Expertise, support, monitoring, and challenge on risk-related matters
THIRD LINE ROLES: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication, coordination, collaboration

Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

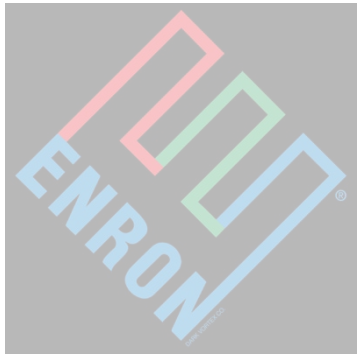
3LoD doesn't hold up to today's demands

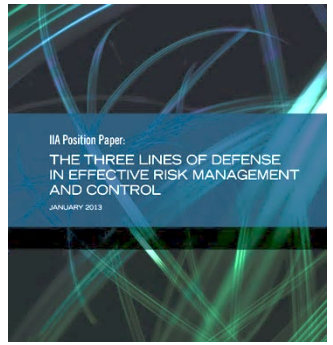
- **Functional, not directional.** Won't steer the organization towards its goals!
- **Inherently siloed.** Creates a tug-of-war between who owns the risk and who owns the budget!
- **Static, not dynamic.** It does not hold up under change!


GOVERNING BODY
Accountability to stakeholders for organizational oversight
GOVERNING BODY ROLES: integrity, leadership, and transparency
MANAGEMENT
Actions (including managing risk) to achieve organizational objectives
INTERNAL AUDIT
Independent assurance
FIRST LINE ROLES: Provision of products/services to clients; risk management
SECOND LINE ROLES: Expertise, support, monitoring, and challenge on risk-related matters
THIRD LINE ROLES: Independent and objective assurance and advice on all matters related to the achievement of objectives
EXTERNAL ASSURANCE PROVIDERS
KEY:
Accountability, reporting
Delegation, direction, resources, oversight
Alignment, communication, coordination, collaboration

Copyright © 2020 by The Institute of Internal Auditors, Inc. All rights reserved.

How did we get here?

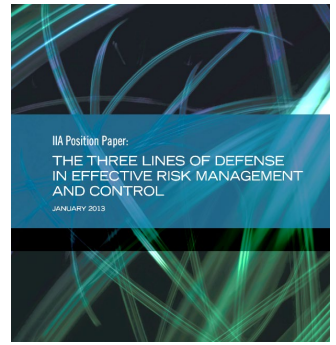




2001 **2002** **2003** **2008** **2013**

How did we get here?

Visit WSJ.com to See Our New Look and Features
THE WALL STREET JOURNAL.
AIG, Lehman Shock Hits World Markets
Focus Moves to Fate of Giant Insurer After U.S. Allows Investment Bank to Fail; Barclays in Talks to Buy Core Lehman Unit
AIG Faces Cash Crisis As Stock Dives 61%



2001 2002 2003 2008 2013

Once daily
NONDESCRIPT
Side effects may include: memory loss, obscure diseases, and fatal allergic reactions

- Great marketing doesn't improve efficacy
- Regulatory support doesn't make it mandatory
- Present popularity doesn't equal long-term success

© Forrester Research, Inc. All rights reserved.

© Forrester Research, Inc. All rights reserved.

© Forrester Research, Inc. All rights reserved.

The world is different now

43%

enterprise risk has increased over the last 12 months[1]

75%

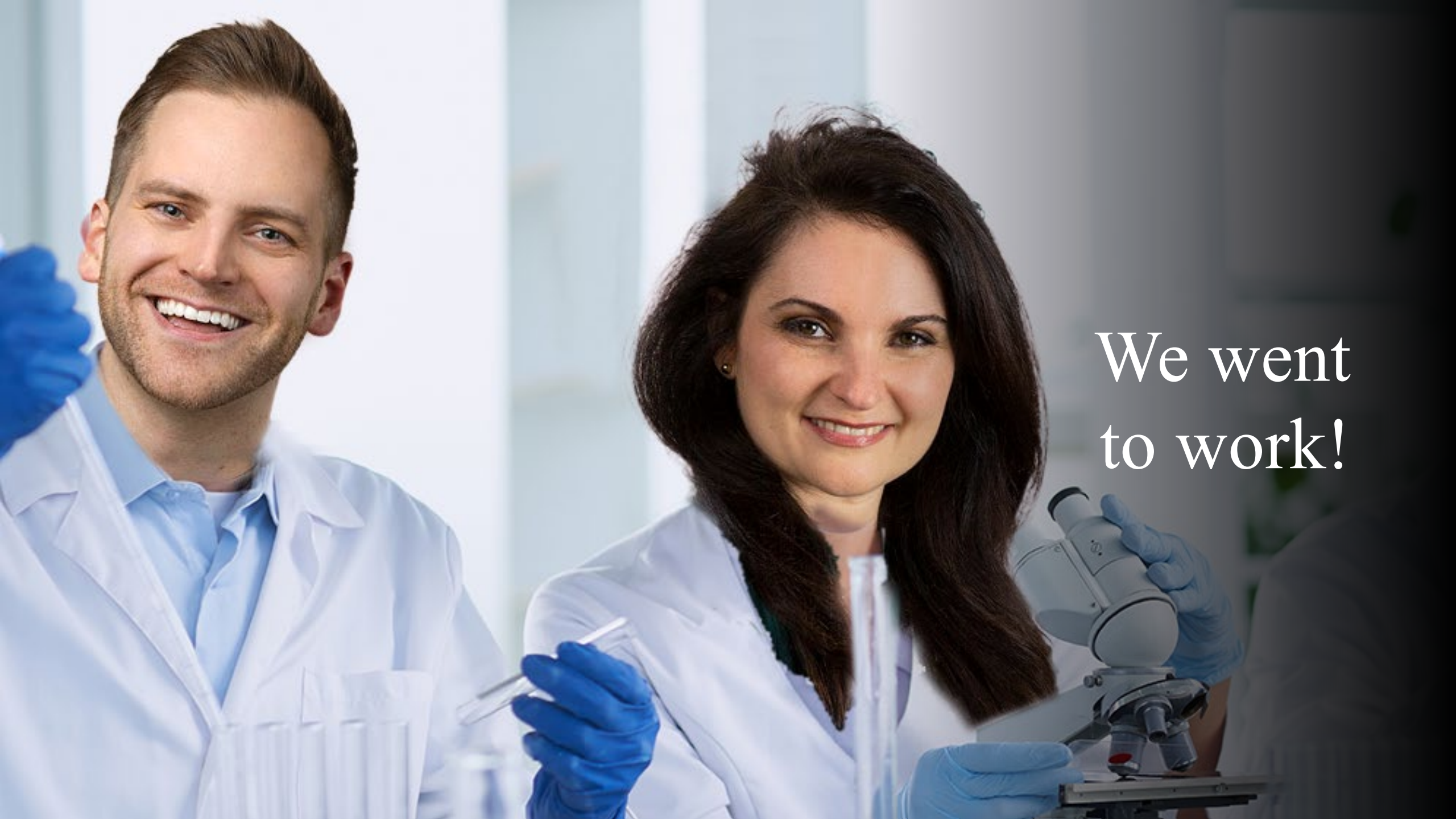
experienced at least one discrete critical risk event in the last 12 months1

52%

experienced at least two breaches in the last 12 months[2]

FORRESTER®

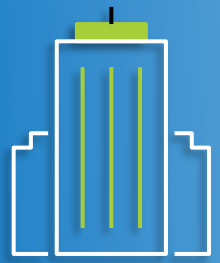
Base 1: 728 enterprise risk management (ERM) decision-makers
Source 1: Forrester's Business Risk Survey
Base 2: 1,488 security decision-makers at enterprise-level organizations (1,000 or more employees)
Source 2: Forrester's Business Risk Survey


We went
to work!

Active ingredients target areas of greatest concern

Addresses ALL risks:

domain agnostic by design



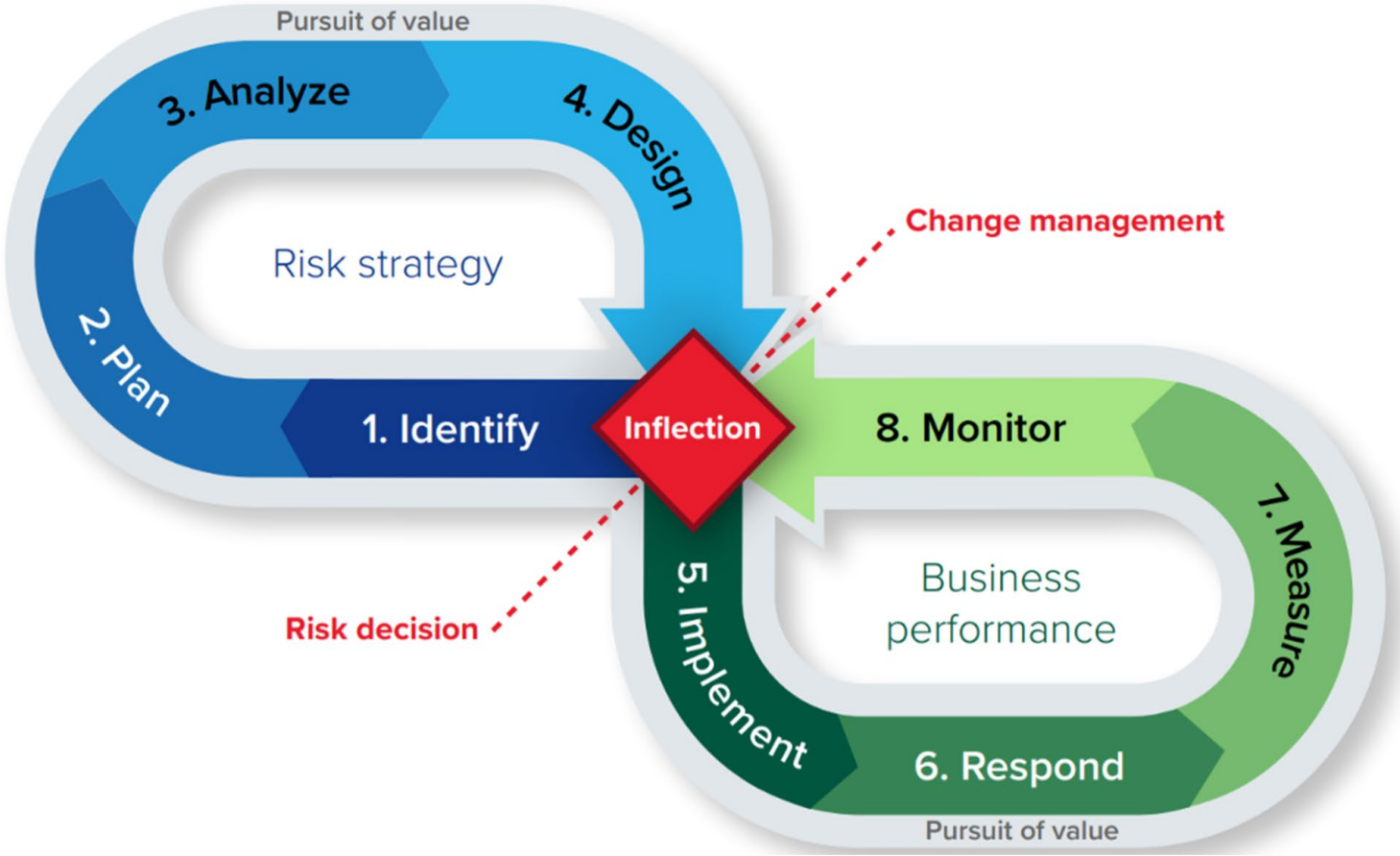
Aligns risk to the business:

bridges strategy with performance

Recognizes opportunity:

built for pursuit of value

Introducing the Continuous Risk Management Model



© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

PHASE 1: IDENTIFY

Identify the opportunity and the business need

- What is your pursuit of value?
- What do you intend to accomplish?
- Establish the business case

PHASE 2: PLAN

Plan the risk strategy and governance approach

- Define the key objectives and milestones to achieve your pursuit of value
- What are the risks associated with meeting those objectives?
- Refine the business case with your initial risk assessment

PHASE 3: ANALYZE

Analyze the business context and feasibility

- Assessment and due diligence
- Translating the goal into an attainable project
- Finalize the business case and initial project plans based on risk-informed inputs

PHASE 4: DESIGN

Design the risk mitigation approach

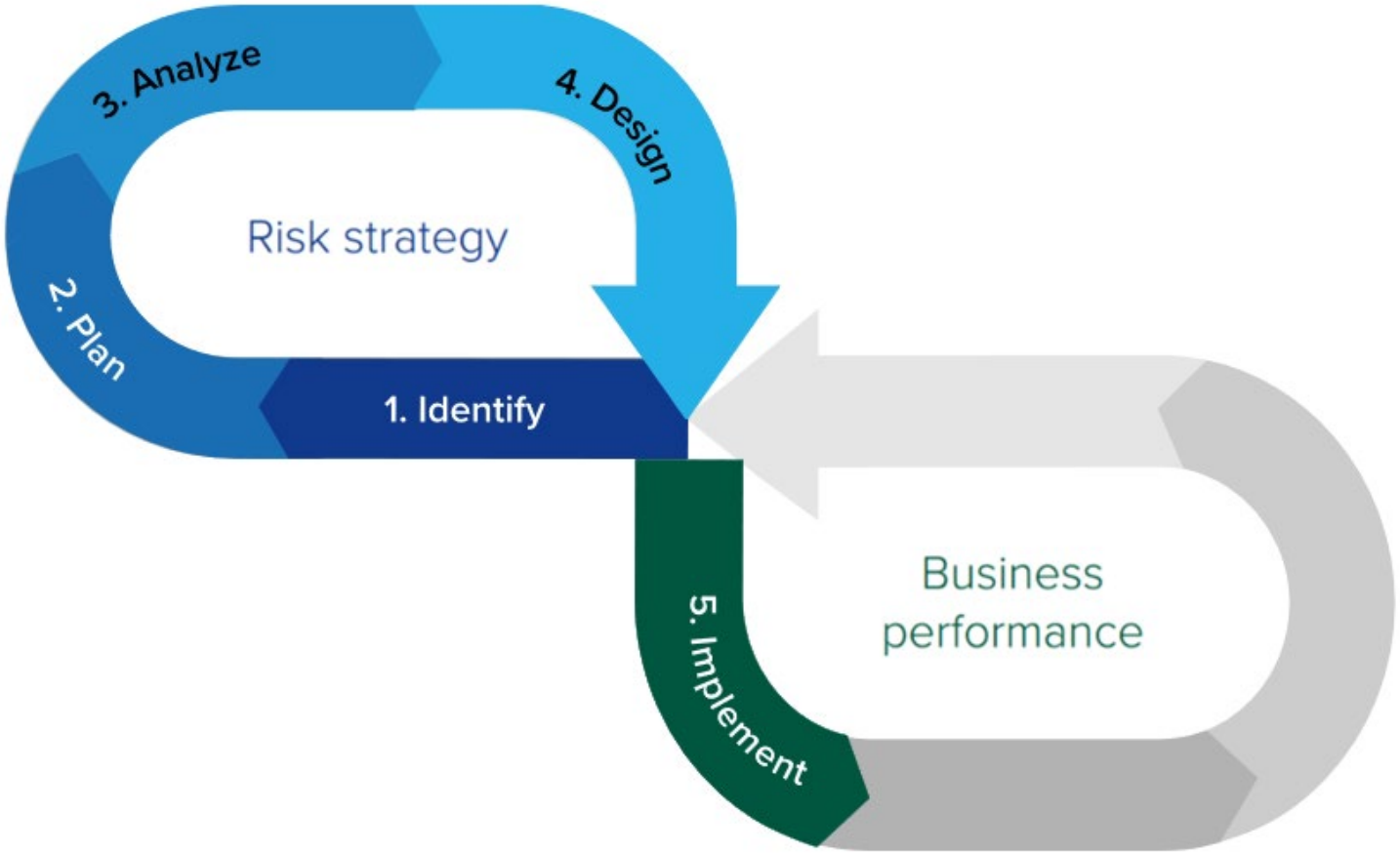
- Identify which risks to accept, transfer, and mitigate
- Incorporate risk mitigation plans into the initial project plan
- Propose an initial control baseline to mitigate identified risks so far

FIRST INFLECTION POINT! RISK DECISION

Risk decisions made earlier

- Risk-based decision to approve the project (pursuit of value) or to go back and revise
- Similar to a formal project approval process – but for risk!
- Communication is key to establish risk and control ownership

PHASE 5: IMPLEMENT



Implement the appropriate mitigating controls

- The tactical work begins
- What is our success criteria for implementing or augment our controls?
- Integrated teams keep the effort aligned

PHASE 6: RESPOND

Respond to deviations from the control baseline

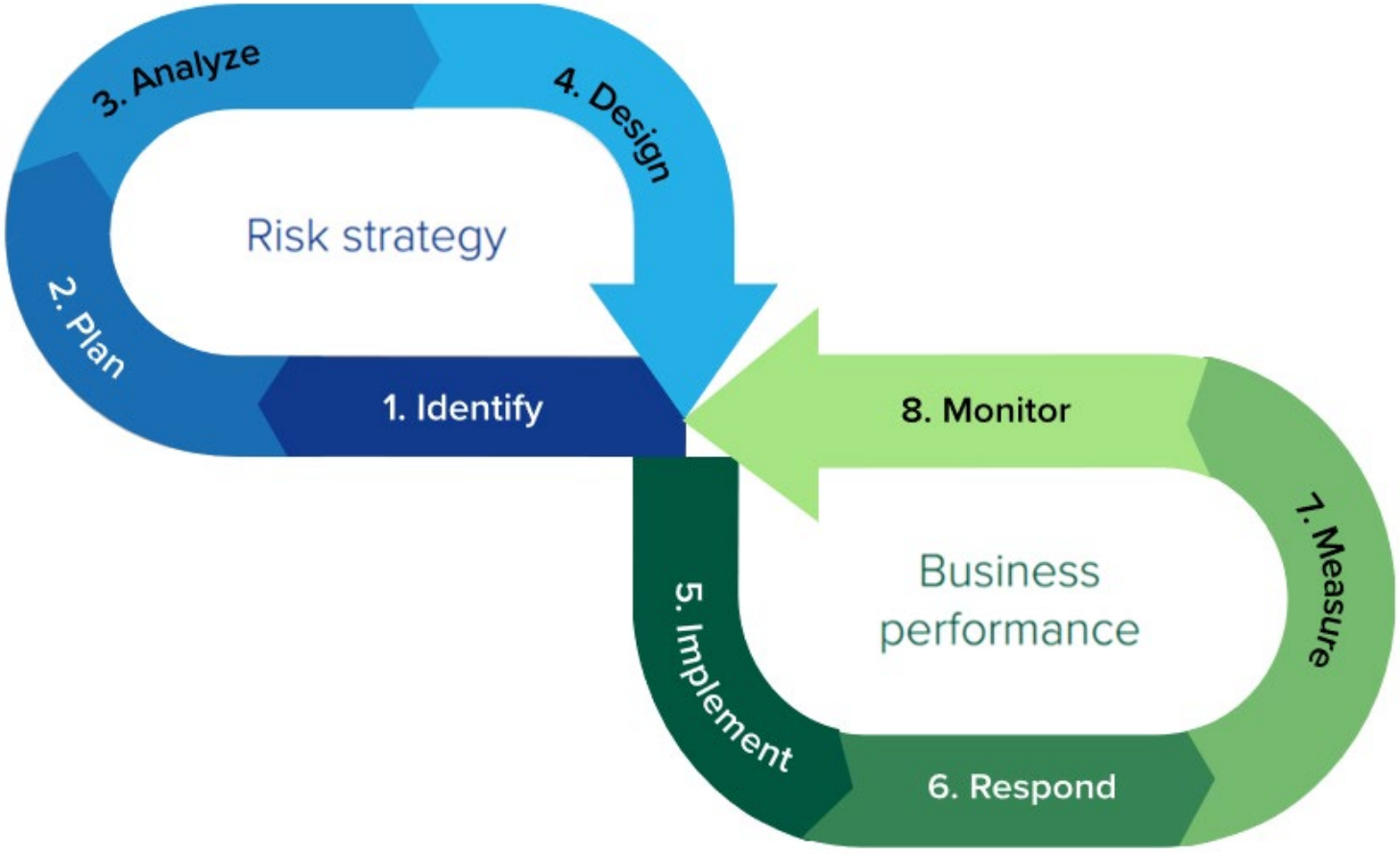
- Change is a constant!
- Are the planned controls still the best option for the job? Has something changed?
- Are additional compensating controls needed?

PHASE 7: MEASURE

Measure control effectiveness against expected outcomes

- You need a risk measurement system
- Control coverage is not enough… how effective are your controls at reducing risk to your pursuit of value?
- Are additional compensating controls needed?

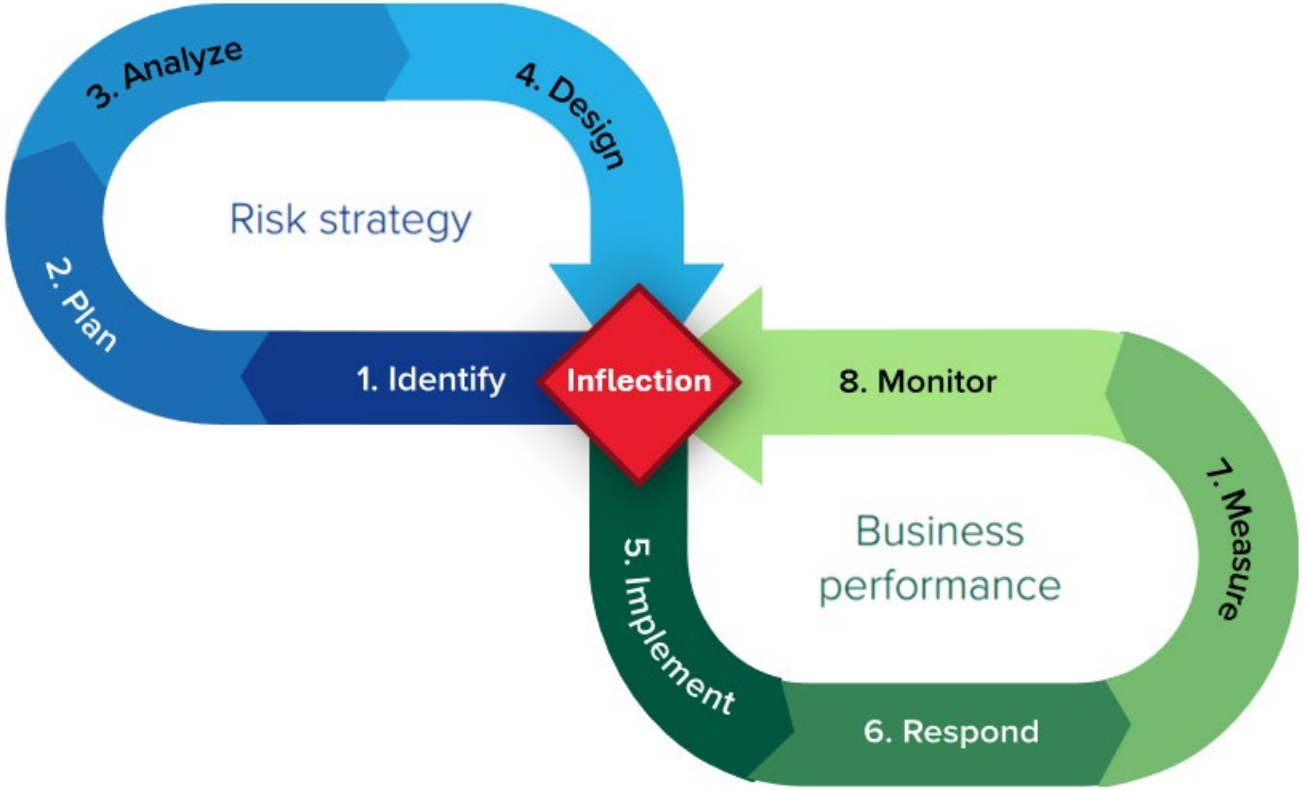
PHASE 8: MONITOR



Monitor continuously and communicate to stakeholders

- What signals, metrics, or indicators can you rely on to know if/when to act?
- How well is your control baseline functioning to reduce risk to an acceptable level for the pursuit of value?

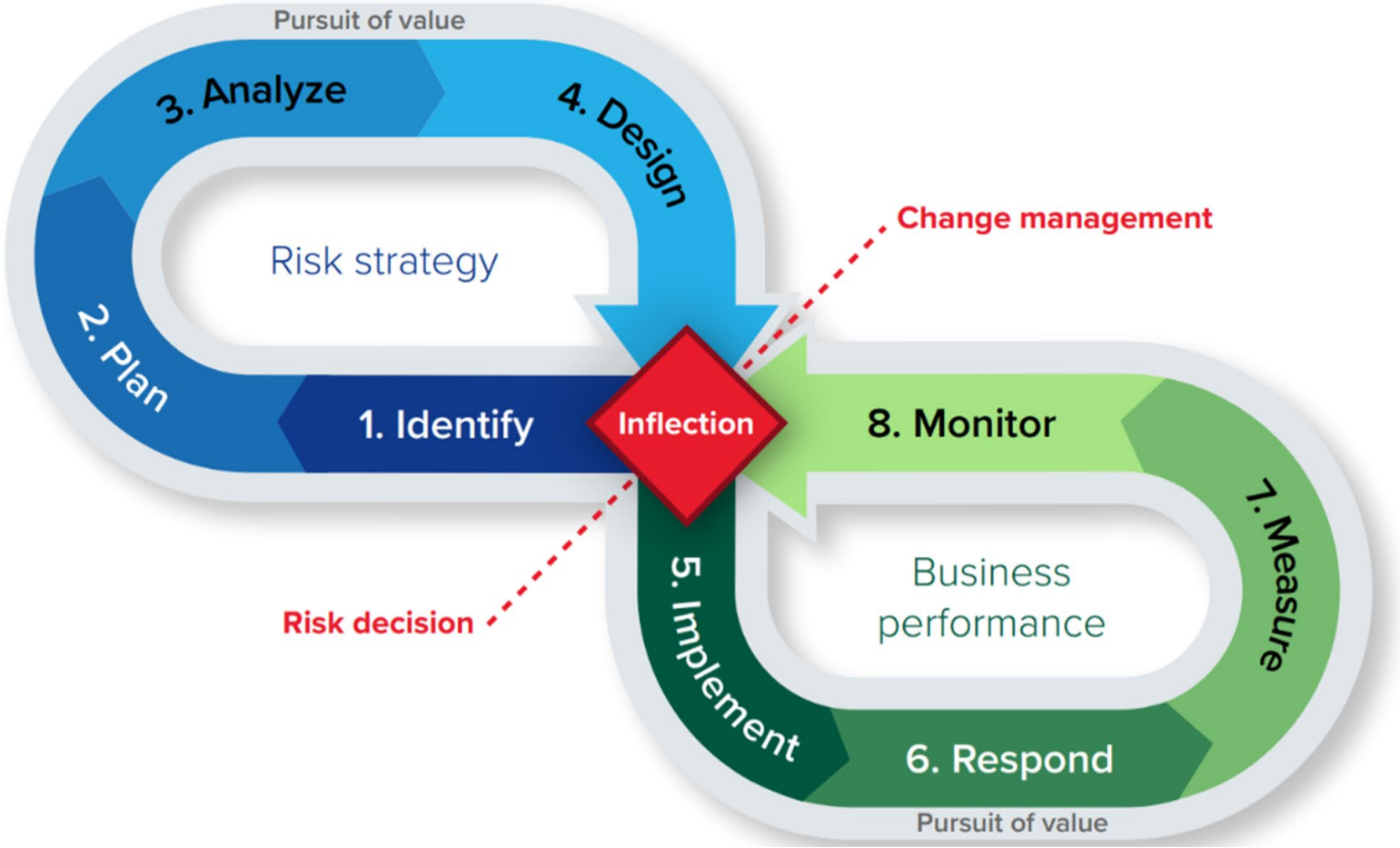
SECOND INFLECTION POINT! CHANGE MANAGEMENT



Your opportunity to make changes

- Change is a constant… and must be managed!
- Avoid the sunk cost trap
- Leverage a risk escalation process
- Are things operating as intended? On schedule? Within budget?

Let's Recap!



© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Align the Continuous Risk Management phases with 3LoD nomenclature

	Phase	Objective	Alignment to 3LOD: Leads	Alignment to 3LOD: Supports
1	Identify	Identify the opportunity and the business need	1	2
2	Plan	Plan the risk strategy and governance approach	1	2 3
3	Analyze	Analyze the business context and feasibility	1	2
4	Design	Design the risk mitigation approach	2	1
5	Implement	Implement the appropriate mitigating controls	2	1 3
6	Respond	Respond to deviations from the control baseline	2	3
7	Measure	Measure control effectiveness against expected outcomes	2	3
8	Monitor	Monitor continuously and communicate to stakeholders	2	3

© Forrester Research, Inc. Unauthorized reproduction, citation, or distribution prohibited.

Recommendations: Start your new regimen today!

Use the Continuous Risk Management model to define your ideal end-state

Mirror your technology workflow to your decision workflow

Use 3LOD to right-size your communication and process structure

Key Takeaways

- Lead with pursuit of value instead of fear of penalties
- Navigate turbulence/uncertainty for resilient outcomes
- Identify upside opportunities and act on them
- Keep pace with speed of innovation

CONTINUOUS RISK MANAGEMENT

Daily treatment for accelerating business, seizing opportunities, and balancing risk management with business performance

Side effects may include:
wild success, better use of time and resources, reduced organizational friction, and better strategic decisions

RSAC™ 2025 Conference

Many Voices.
One Community.